AN EMERGING THREATS ESSAY

Cybersecurity and Public Goods

The Public/Private "Partnership"

by Paul Rosenzweig

Koret-Taube Task Force on National Security and Law
www.emergingthreatsessays.com

task force on national security and law

In January 2010, Google released disturbing news: It had been the subject of a "highly sophisticated and targeted attack" that had originated in China, resulting in the "theft of intellectual property" from Google. The attack seemed to be targeted at Chinese human rights activists. And Google was not alone—at least twenty other major companies spanning sectors including Internet, finance, and the chemical industry were also targeted.[1] At its core, the attack apparently attempted to corrupt some of Google's source code.

Though it is notoriously difficult to confirm responsibility for cyber intrusions, there seems to be little doubt that official Chinese authorities were behind the attack. Indeed, one of the classified State Department cables released by WikiLeaks reports that the operation was authorized by the Politburo Standing Committee,[2] which is roughly equivalent in authority to America's National Security Council. The intrusion seems, therefore, to be of a piece with China's notorious efforts to maintain control over its citizens' Internet access and is, in many ways, unsurprising.

Far more surprising, however, was Google's next step: it turned to the National Security Agency (NSA) for help.[3] Google sought to take advantage of the NSA's expertise in "information assurance." In other words, it wanted the NSA to help it evaluate the vulnerabilities in its hardware and software and assess the intruders' level of capability. Using NSA expertise, Google would have a better understanding

This paper will appear in modified form as a chapter in the forthcoming book, *Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (Praeger 2012) by Paul Rosenzweig.

HOOVER INSTITUTION
STANFORD UNIVERSITY

of how its systems were penetrated. Google, in turn, would share with the NSA any information it had about the precise nature of the malware code that was used to corrupt its system.

This cooperation agreement between Google and NSA is notable for a number of reasons. First, Google turned to the NSA for assistance and not to the Department of Homeland Security (DHS), which has the nominal responsibility for assisting in the protection of private sector infrastructure. Second, the more fundamentally transformative aspect of the agreement is that Google looked to anyone in government at all for assistance.

Google's business model is controversial in Silicon Valley. But whatever one thinks of its commercial approach, nobody doubts its technical expertise. Google—along with other major cyber actors such as Facebook and PayPal, service providers like Verizon, and software manufacturers like Microsoft—is at the forefront of cutting-edge cyber innovations. Yet even with that deep and sophisticated base of knowledge, Google was impelled to seek governmental assistance.

Informally, private sector leaders in the IT/Telecoms space often say they don't need anything from the government.[4] Indeed, their repeated refrain is often that government involvement will stifle innovation rather than foster security. As we shall see, that argument has great appeal. Yet one of the most sophisticated players in the entire domain, Google, turned to the government for help. What does that say about the desirability of public/private cooperation in cybersecurity?

From the government's perspective, the need for robust and effective cooperation seems self-evident. It is commonplace to note that private entities own and operate 85–90 percent of the cyber infrastructure—though no authoritative source for this figure can be found.[5] Most government cyber traffic travels on non-governmental cyber systems. And those systems, in turn, are used to control or communicate with a host of other critical infrastructures—the transportation system, the electric grid, the financial markets, and the like. Thus, core national security functions of command, control, communications, and continuity are all dependent, to greater or lesser degrees, on the resilience of the private-sector networks. As a result, it would seem that the federal government must be deeply concerned with private-sector cybersecurity.

Yet public and private actors often do not coordinate well together. The challenge for the federal government is how to integrate its efforts with those of the private sector. To date the results have been less than stellar, at least in part because of private-sector resistance to the concept.

Cybersecurity Effectiveness—Is It Working Today?

The Internet is a very unique place. Unlike most human phenomena, it is not bounded in space and it has no physical borders. Its structure is outside of our common experience: even though most lay observers think of it as something like the telephone network, its structure is actually quite different. While the telephone networks are "hub and spoke" systems with the intelligent operation at the central switching points, the Internet is truly a "world wide web" of interconnected servers where the intelligent operations occur at the edges (in our mobile devices and laptops running various "apps"). At its central core, the Internet packet switching protocol is fundamentally pretty dumb.[6]

This fundamental architecture of the Internet gives rise to two factors that are, in effect, built into the system. The first is the problem of anonymity. Given the vastness of the web, it is quite possible for those who seek to do harm to do so at a distance, cloaked in the veil of anonymity. While that veil can be pulled aside, doing so requires a very great investment of time and resources, making malfeasant actors immune, for all practical purposes, from swift and sure response or retaliation. The second factor is the difficulty of distinction. Any successful cyber attack or intrusion requires "a vulnerability, access to that vulnerability, and a payload to be executed."[7] But in practice the first two parts of that equation (identifying a vulnerability and gaining access to it) are the same no matter what the payload that is to be delivered. Thus, for those attempting a defense, it is virtually impossible to distinguish *ex ante* between different types of intrusions because they all look the same on the front end: cyber espionage, where the intrusion is a payload that seeks to hide itself and exfiltrate classified data; cyber theft, where the object is stealing unclassified financial data; and a full-scale cyber attack, where the payload left behind may lie dormant for years before it is activated and causes grave cyber damage. The difference arises only when the effects are felt. The closest kinetic world analogy would be something like never being able to tell whether the plane flying across your border was a friendly commercial aircraft, a spy plane, or a bomber.[8]

Taken together, these two factors make cyber systems highly vulnerable to attack. Indeed, some people say effective cybersecurity is more of a dream than a reality because cyber attacks routinely defeat cyber defenses and that is likely to continue for the foreseeable future. In short, life in the cyber domain is thought of as Hobbesian in nature—often "solitary, poor, nasty, brutish and short."[9] But how accurate is this portrayal? What, if anything, can we say about the delivery of cybersecurity as an empirical matter? How effective are our efforts?

Sadly, though the question is a vital one, there is little data to drive effective policymaking. For instance, the US-Computer Emergency Readiness Team (US-CERT)

Monthly Activity Report for April 2011 does not recount activity involving cyber intrusions, attacks, and thefts—as one might expect it to—but, rather the activities of US-CERT itself: how many reports it has issued.[10] Given that US-CERT is "charged with providing response support and defense against cyber attacks for the .gov network and information sharing and collaboration with state and local government, industry and international partners," the lack of data on the necessity of its efforts (much less their efficacy) is troubling.

The problem is not limited to the intrusion detection realm. It also pervades efforts to measure actual effects. As three authors from PayPal recently noted, "Estimates of the magnitude and scope of Cybercrime vary widely, making it difficult for policymakers and others to determine the level of effort to exert in combating the problem."[11] While individuals, companies, and trade associations have disparate pieces of the information puzzle, the data on cybercrime has never been convincingly aggregated. And what is true of cybercrime is true, to an even greater degree, of instances of cyber espionage (of both the industrial and sovereign variety).

To be sure, some reports are more substantive than the US-CERT data, but they provide limited insight. For example, in 2010, the Internet Criminal Complaint Center (IC3) received 303,809 complaints of Internet crime.[12] Likewise, DHS reported 5,499 intrusions into U.S. government computer systems in 2008.[13] Neither of these numbers illuminates the scope of the problem because the unreported and undetected instances of crime or intrusion are, by definition, unknowable. Indeed, these modest numbers pale next to other more apocalyptic estimates of malfeasant activity on the Internet: Deputy Secretary of Defense William Lynn says military systems are "probed thousands of times and scanned millions of times" every day.[14]

While more concrete estimates of the economic costs of cyber crime and cyber intrusions are available, and offer some indication of the scope of the problem, they are highly conjectural. For example, the consulting firm Detica has estimated the annual loss from cyber intrusions in the United Kingdom at £27 billion.[15] Two years earlier, McAfee Security estimated the annual cyber crime losses at $1 trillion globally.[16]

These estimates may well be inflated by their methodology. The bulk of the losses are estimated to flow from the theft of intellectual property (some form of industrial espionage), with actual monetary loss believed to be an order of magnitude less (i.e., £3.7 billion annually in the U.K. from fraud and identity theft).[17] If the same factor were applied to the McAfee global number, the annualized monetary loss worldwide would be $100 billion—a significant number, but by no means astronomical. More notably, these numbers are a rough estimate at best—and they produce figures that

are inherently suspect. At least one critic, for example, has characterized the Detica study as "nonsense" and "a grubby little piece of puffery."[18]

Perhaps somewhat more authoritatively, the Government Accountability Office (GAO), repeating an estimate made by the Federal Bureau of Investigation (FBI), believes that in 2005 the annual loss due to computer crime was approximately $67.2 billion for U.S. organizations. The estimated losses associated with particular crimes include $49.3 billion in 2006 for identity theft and $1 billion annually due to phishing.[19]

Another way of trying to estimate the scope of the cybersecurity problem would be to examine how much is spent in preventing intrusions and theft—after all, nobody would expect rational businesses to spend more in prevention than they anticipate in losses. In 2010, the Ponemon Institute surveyed forty-five major American companies and found that the median amount they spent annually on cybersecurity was $3.8 million, or a total of $135 million for these companies.[20] No convincing extrapolation from this data has been (or, frankly, is likely to be) made, but they do suggest that the threat is considered rather more modest than existential.

One massive study of Internet traffic conducted for Bell Canada demonstrates both the scope of the problem and the difficulty in definitively assessing its severity.[21] The study reviewed 839 petabytes of data,[22] containing over 4 billion emails each month, and carrying more than $174 billion (in Canadian dollars) of commerce every day. Within this flood of data, more than fifty-three gigabytes per second contained malicious code of some sort. The investigators observed on the order of 80,000 zero-day exploits per day and estimated that more than 1.5 million compromised computers attempted more than 21 million botnet connections each month.[23] This data is more or less consistent with estimates by large cybersecurity companies: Symantec, for example, discovered 286 million new unique malicious threats in 2010, or roughly nine new malware creations every second.[24] And yet, from all this, the most that can be said is that a large number of financial transactions are at risk—data about actual harm remains painfully elusive.

From this data, we can reach one firm conclusion and one tentative one. The firm conclusion is that the federal government needs to undertake the difficult task of developing a useful data set on the scope and effect of cyber intrusions and cyber crime. No such metrics exist today, and good policy is difficult to make in a data vacuum.

Both the United States and Europe seem to recognize this critical gap.[25] Each is moving toward a mandatory data reporting regime that would require private sector actors to report some intrusions into their systems. In the United States, the Obama administration has proposed a mandatory data breach notification law that would,

for significant breaches, require notification both to the individuals affected and to the federal government.[26] Likewise, in 2009 the European Union adopted a directive relating to the telecommunications industry. Its Article 13a would require all electronic communications providers to report on security breaches to the European Network and Information Security Agency (ENISA).[27] While neither proposal has yet been implemented (the EU directive requires enactment by each member state, and the Obama plan is still only a proposal) both could ultimately provide a better factual understanding of the nature of security breaches. Notably, however, both these programs would collect data mostly about breaches and intrusions; only limited data about the actual consequences of any security breach would be collected.

The second, more tentative conclusion given the data available thus far is that the broad overall economic impact of cyber intrusions and cyber crime is likely significant but not insurmountable. Clearly some harm is occurring, otherwise actors would not engage in the profitless conduct of protecting against it, but the magnitude of that harm remains unclear.

Cybersecurity as National Security

One important caveat to the foregoing is in order: this data and the attendant conclusions are only relevant to assessing the economic impacts of cyber crime and cyber espionage. No fair estimate can be made about the impact on national security of a singular or significant cyber event.

To cite one incident, consider the recently-analyzed GhostNet malware.[28] That malware imported a Trojan horse program onto infected computers, which allowed a remote user to, effectively, control the computer. The remote user could activate a keystroke logger, turn on the computer's video camera or microphone, and, of course, exfiltrate any data stored on the computer. First observed on computers operated by the Dali Lama, the malware was found in dozens of other computers, including some located in the embassies of India, Malaysia, and Indonesia, ministries of foreign affairs, and even on an unclassified system at NATO (SHAPE) headquarters. Extended analysis eventually traced the malware to an IP address on Hainan Island off the coast of China—an island that, perhaps coincidentally, is home to the headquarters of China's signals intelligence agency.

It is difficult to assess how significant such an incident might have been. It is even more difficult to conduct a realistic assessment of the risks of further espionage activity, much less the risks that might have physical effects. Last year, for example, a piece of malware known as Stuxnet significantly affected the capabilities of the Iranian nuclear program.[29] The origin of Stuxnet is unknown, though many speculate that the Israelis developed it, with American assistance.[30] Whatever its source, Stuxnet demonstrated

that incorporeal software can have real-world, kinetic effects. We now face the prospect of cyber attacks that destroy real things, like perhaps the electric grid.

Policy considerations about these sorts of national security vulnerabilities turn not on reviewing data about ongoing criminal intrusions, but on assessing the likelihood of such an event by measuring potential threats, vulnerabilities, and consequences. The little data we have addresses, inferentially, the vulnerability aspect of that question: from intrusions, we can learn where the holes are. We may also collect some data about consequence, especially when the effect on the infrastructure can be measured, but that data is difficult to quantify. What, for example, were the consequences to society of the hacker group Anonymous's attack on PayPal, Mastercard, and Amazon? In the end, no solid data on the threat exists—we can only measure capabilities, and then only by educated guess work. We have no clear sense of true intent. As a result, we lack a solid, quantifiable risk assessment of the cyber threat to national security and this leaves policymakers with only a speculative guess as to the extent of our risk from a cyber attack by a willful cyber opponent.

An Introduction to the Economic Theory of Cybersecurity

In considering the appropriate scope for government intervention in the cyber domain, we must examine first principles and consider a theoretical model for when governmental activity is warranted. The theoretical model need not govern decision making, but can serve as a useful guidepost for examining the question.[31]

As a matter of theory and of ideological commitment—born of the independence inherent in the foundations of the Internet—most private sector leaders say there is no need for much, if any, government assistance in the cybersecurity market. All they require is for government to enable the sharing of more information by clarifying legal uncertainties (described more fully in the next section) and then get out of the way. However, a closer examination of the theoretical argument suggests significant room for governmental engagement and, indeed, helps to explain why Google went to the NSA.

The theory runs something like this: a public good is one that is both non-rivalrous and non-exclusive.[32] In other words, its use by one person does not affect its use by others, and its availability to one person means it is also available to every other person. The classic example of a public good is national defense. Providing defense services to protect one citizen does not diminish the protection enjoyed by another citizen, and defense services provided to one citizen are enjoyed by all other citizens. By contrast, private goods—a pair of shoes, for instance—can only be used by one person at a time, and their use by one person makes them unavailable to others.

	Non-Rivalrous (use by A does not affect use by B)	**Rivalrous** (use by A affects use by B)
Non-Exclusive (use by A does not prevent use by B)	*Public Goods* National Defense Clean Air Cybersecurity Threat Information	*Common Pool Goods* Fishing Grounds Parks Early Internet
Exclusive (use by A prevents use by B)	*Club Goods* Private Club Movie Theater Secure Network	*Private Goods* Shoes Automobiles Cybersecurity Firewalls and Intrusion Detection Systems

Public goods are typically beset by two problems: free riders and assurance. Free riders are individuals who hope to reap the benefits of a public good but refuse to contribute to its creation because they think others will do so even absent their participation. The assurance problem exists when people refuse to invest in the production of a public good because they believe there will never be enough cooperative investment to produce the good and, thus, that their investment would be futile.

The classic solution to this conundrum is governmental intervention. When the citizenry views a public good as necessary but cooperation is unavailing, its government may choose to coerce people to cooperate through taxation or some other mandate and provide the public good.

Security Information as a Public Good

Security in cyberspace, like physical security in the kinetic world, is a market good. People will pay for it, and pay quite a bit. But security in cyberspace is not a singular good—rather it is a bundle of various goods, some of which operate independently and others of which act only in combination. Broadly speaking, these goods are purchased in an effort to protect networks, hardware, data in transit, and stored data from theft, destruction, disruption, or delay.[33]

Given the vast scope of cybersecurity goods, it is no surprise that different aspects of the bundle may be provided by different sources. Just as some security in the physical world can be purchased directly in the private market, many security systems in cyberspace, such as anti-virus software and intrusion-detection systems, are private goods, bought and sold between private-sector actors. They are rivalrous, because their use affects other actors, and excludable, since their owner can limit their use by others. Indeed, evidence from the financial sector suggests that cybersecurity is, to a very large degree, a private good, adequately provided by the private sector.[34]

There is, however, one aspect of the bundle of cybersecurity goods that is clearly a public good—information about threat and vulnerability.[35] Such information is both non-rivalrous (giving it to one person to use does not affect how another might use it) and non-exclusive (everyone can use the information when it is made available). As a result, we are seeing greater focus on laws and regulations regarding information sharing because our legal mechanisms have not adequately captured the nature of the information being shared, and are thought to be impeding rather than enhancing the wide distribution of this public good. This view of threat information as a public good also explains, at least partially, why Google might look to NSA for assistance. The company seeks a public good, namely information about threats to its systems.

This insight into the nature of security information is also consistent with a micro-economic understanding of the incentives that convince an individual actor to disclose information about threats and vulnerabilities in its system. There are a host of reasons why private-sector actors may be reluctant to make such disclosures, including the risk of damaging their reputation and their customers' trust, incurring liability and indemnification claims, suffering negative effects in the financial markets, signaling weakness to adversaries, and harming job security and individuals' career goals.[36] Treating information as a public good tends to overcome these factors.

Private Good, With Externalities

Even if cybersecurity is a private good, however, government may still have a role in its production. The production of a private good will often cause an externality—that is, the activity between two economic actors may directly and unintentionally affect a third party. Externalities can be either positive (when a transaction I voluntarily enter into benefits a third party who pays nothing for the benefit) or negative (when the transaction harms the individual).

Many cybersecurity activities have positive externalities. By securing my own server or laptop against intrusion, for example, I benefit others on the network whose systems become more secure by my actions. Indeed, almost every security measure performed on any part of cyberspace improves the overall level of cybersecurity by raising the costs of attack.[37]

But cybersecurity also has two negative externalities. The first is a diversion effect: some methods of protection, such as firewalls, divert attacks from one target to another, meaning one actor's security improvement can decrease security for systems that are not as well-protected.[38]

The second is a pricing problem: private sector actors often do not internalize the costs of security failures in a way that leads them to take adequate protective steps. When

software fails to prevent an intrusion or a service provider fails to interdict a malware attack, there is no mechanism through which to hold the software manufacturer or Internet service provider responsible for the costs of those failures. The costs are borne entirely by the end users. In this way, security for the broader Internet is a classic market externality whose true costs are not adequately recognized in the prices charged and costs experienced by individual actors.

Addressing the dual nature of these cybersecurity externalities poses a significant policy challenge. Both cases suggest a role for government. But identifying which externality predominates is essential, since the two types point to different policy solutions. We typically subsidize private goods that cause positive externalities because not enough of those goods exist and we wish to encourage investment. By contrast, we often tax or regulate private goods that cause negative externalities to compel the original actor to internalize some of the external costs and reduce the level of production to one commensurate with its true costs.

In either case, two broad caveats to government involvement in the private sector's provision of cybersecurity merit note. First, as with any governmental interference in the marketplace, public choice theorists doubt the government's ability to systematically make the right choices, reasoning that rent-seeking behavior by an economic actor seeking a regulatory or legislative preference will adversely affect decision-making.[39] They believe subsidies, taxes, and regulations will not foster the "right" result, but rather the result that concerted lobbying efforts favor—a concern not unique to the cyber arena.

Second, the pace of technological change has increased exponentially—a factor that is perhaps unique to cybersecurity. But the government's hierarchical decision-making structure allows only slow progress in adapting to this phenomenon and operates far too slowly to catch up with the change. Our policymaking apparatus cannot turn inside the cyberspace innovation radius: as one colleague has put it, the government is using a "Ford sedan" policymaking system to manage the cyberspace "Porsche" system.[40] Thus, though one may acknowledge the theoretical ground for government regulation of cybersecurity based on the externalities that exist, one may doubt the government's capacity to exercise its authority in a timely manner to successfully deal with the problems. Put bluntly, by the time the government closes its notice and comment period and reaches a decision, the technology at issue will likely be obsolete.

Self-Governing Structures

This does not, however, suggest the possibility of strong private sector self-regulation. As international security scholar Joseph Nye has argued, cyberspace may be also characterized as a "common pool resource."[41] Common pool resources are ones, like a

fishing ground, where exclusion of users is difficult and the resource is subtractable, or rivalrous, such that use by one person diminishes the availability of the resource to another. The physical bandwidth and servers that make up the Internet may well be considered a common resource, as anyone who follows the "net neutrality" policy discussion well understands.[42]

In some limited circumstances, common pool resource users can self-organize and act collectively to govern the resource use.[43] One well-known example of this involves the collective regulation of lobster catches by Maine lobstermen.[44] But this type of self-governance can arise spontaneously only when the number of users is relatively few and the reputational costs of violating social norms are high. While that may have described the Internet at the dawn of the computer age (the first network had only four nodes on it), it hardly describes the cyber domain today. At this point, cyberspace is so diffuse that a truly successful self-governing structure is hard to imagine.[45] The resource is too large, there are too many users, and the dynamics of its governance are highly unpredictable.[46]

▪ ▪ ▪

Thus while some information-based elements of cybersecurity can be fairly characterized as public goods, the remaining elements are either private goods with recognized externalities and grave challenges for government regulation, or common pool resources with equally grave challenges for private sector coordination. For the latter two categories of goods, devising an appropriate public policy is truly a "wicked problem."[47]

Information Sharing, Public Goods, and the Law

This economic understanding of cybersecurity suggests why a significant fraction of the policy debate about cybersecurity and public/private partnerships revolves around the challenge of effectively sharing security information. Some people insist that existing legal restrictions prevent the private sector from creating cybersecurity. They say some restrictions weaken the government's ability to adequately share threat information with the private sector, while others limit how the private sector shares information with the government or amongst itself. In other words, the "received wisdom" is that our collective response to new threats is limited by law—the government can't share some threat information about new malicious software with the private sector because of classification rules, and privacy rules prevent private sector actors from sharing the same information with the government or their peers.

The focus on information sharing makes sense when seen through the prism of our theoretical model: because threat and vulnerability information may have

characteristics of a public good, it is in society's interest to foster their creation and distribution. If existing laws did, in fact, restrain and restrict those aims—if classification and privacy laws limited information sharing—that would be a policy dissonance. However, on closer examination, many of these legal limitations may be less constricting than they are perceived to be. In the end, what really restricts cooperation are the inherent caution of lawyers who do not wish to push the envelope of legal authority and/or policy and economic factors such as proprietary self-interest that limit the desire to cooperate.

The information in question will relate, broadly speaking, either to specific threats from external actors (for example, knowledge from an insider that an intrusion is planned) or to specific vulnerabilities (for example, the identification of a security gap in a particular piece of software). In both situations, the evidence of the threat or vulnerability can come in one of two forms: either non-personalized information related to changes in types of activity on the network, or personalized information about the actions of a specific individual or group of individuals.[48] Needless to say, the sharing of the latter category of Personally Identifiable Information (PII) is of greater concern to civil libertarians than the sharing of network traffic information.[49]

Information Sharing from the Government to the Private Sector

Some suggest that the principal barriers to an effective public/private partnership in combating cyber threats are limitations on the government's ability to share threat and vulnerability information with the private sector. Sometimes the government has collected this information using sources and methods that are classified, and disclosure of the information risks compromising those sources and methods. Less frequently, the existence of the threat or vulnerability is itself classified information, since disclosure of its existence or scope might adversely affect security.

In general, classification rules serve a salutary purpose—they protect information whose disclosure "reasonably could be expected to cause exceptionally grave damage to the national security."[50] That instinct against disclosure, however, conflicts with a newer post-9/11 standard of enhanced information sharing. In the realm of cybersecurity, these conflicting impulses are a constant source of tension.

For example, the Government Accountability Office reported last year that a survey of private sector actors showed that what they want most is for their federal partners to provide "timely and actionable cyber threat and alert information—[that is,] providing the right information to the right persons or groups as early as possible to give them time to take appropriate action." However, "only 27 percent of private sector survey respondents reported that they were receiving timely and actionable cyber threat information and alerts to a great or moderate extent."[51] Likewise, private sector actors

report that they do not routinely receive the security clearances required to adequately receive and act upon classified threat information.[52]

For the most part, these problems are ones of policy, rather than law. No legal barrier prevents provision of the requisite security clearances—it is simply a matter of inadequate resources. Likewise, the untimeliness of US-CERT's alert process is more the product of the need for internal review and the government's insistence on accuracy over timeliness than it is of any legal barrier to sharing. And, indeed, this policy choice may be the right one, since inaccuracy will erode the government's credibility—but the cautious impulse still makes government information sharing less effective.

Still, there may be some legal restrictions beyond classification that do interfere with information sharing. According to the GAO, DHS officials report that "US-CERT's ability to provide information is impacted by restrictions that do not allow individualized treatment of one private sector entity over another private sector entity—making it difficult to formally share specific information with entities that are being directly impacted by a cyber threat."[53] The apparent need to avoid the appearance of favoritism amongst private sector actors may be a barrier that needs re-consideration (though this reference is the only time the author has seen this problem identified, raising a question about its general applicability).[54]

Even this limited legal prohibition seems to have had little practical effect. As Google's request for assistance to the NSA demonstrates, there are plainly situations in which company-specific assistance can be rendered by the government. Indeed, the Google experience is in the midst of being generalized. Recently the Department of Defense announced the continuation of a pilot project wherein it would share threat signature information with Internet Service Providers (ISPs) which, in turn, would use that information to protect the systems of private corporations that are part of the Defense Industrial Base (DIB).[55] This pilot program is voluntary and involves only the one-way transfer of information from the government to the private sector—a structure that alleviates most, if not all, of the legal concerns about government surveillance activities.[56] More broadly, the Obama administration's draft cybersecurity proposal would codify authority for DHS to provide assistance to the private sector upon request.[57] Thus, these problems are not likely to be ones of law, but of commitment.

Private-to-Private and Private-to-Government Sharing

Consider next the privacy laws that are often said to limit the private sector's ability to cooperate with the government or amongst itself. Two portions of the Electronic Communications Privacy Act (ECPA) apply here.[58] The first is Title I, relating to wiretapping and sometimes referred to as an amendment to the Wiretap Act.[59] The second is Title II, relating to the privacy of electronic communications and often called

the Stored Communications Act (SCA).[60] These laws were created to protect privacy and to impose checks and balances on law enforcement access to private citizens' communications. As such, they serve important public policy goals.

But the laws are no longer applicable to current conditions. Passed initially in 1986, they were largely drafted to address issues relating to the telephone network and have yet to be fully modernized to deal with today's Internet-based communications technologies. Some Internet service providers argue they can't effectively protect customers and networks because the laws' ambiguity creates legal uncertainty about whether service providers can use certain communications information to protect consumers and/or share certain information voluntarily with the government for purposes of cybersecurity.

They argue that changes are necessary in the laws to clearly authorize cooperative cyber activities. The SCA, for example, generally prohibits an electronic communications provider or a remote computing services provider from disclosing the contents of electronic communications or information about a customer who subscribes to its services, absent appropriate legal process. Likewise, the Wiretap Act prohibits the interception of communications in transit, except with legal authorization. Service providers say these general prohibitions inhibit sharing of cyber-related threat information.

The arguments for ambiguity are, however, somewhat overstated. Both laws have exceptions related to the protection of service provider networks. The SCA permits information to be divulged "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service."[61] The phrase has rarely been interpreted by the courts, and the one notable case that did so rejected Apple's argument that the phrase authorized the company to comply with a civil subpoena, since failing to do so would cause it to lose money.[62] But there is no reason to suppose that the phrase "protection of property" does not encompass protection of the network that the service provider maintains. To be sure, this requires a slight interpretive leap, but it is slight enough that it is difficult to understand the legal hesitancy of network providers on this score.

Indeed, this "provider protection" language is copied from the provider exception of the Wiretap Act,[63] whose meaning is reasonably well settled. The provider exception of the Wiretap Act gives a provider the right to conduct reasonable, tailored monitoring of the network to protect the provider's property from unauthorized use and for other legitimate provider reasons, as well as to disclose communications intercepted.[64]

Thus, the seeming uncertainty attending the law is rather overblown.[65] There is, however, some room for question. The ambiguity lies in the scope and frequency of the information sharing. The relevant provisions permit a "tailored" approach and may not necessarily be read to authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To interpret those provisions so broadly might be inconsistent with the promise of privacy that undergirds the Wiretap Act and SCA. And yet, routine sharing may be precisely what is necessary to effectively protect the networks. Pity the service provider who is trying to determine when his permissibly "tailored" sharing becomes impermissibly "routine."

There are other possible answers, of course. For example, both the Wiretap Act and the SCA have consent provisions permitting disclosure or interception in situations where the customer has consented.[66] Relying on these provisions, it would appear that service providers are authorized to collect, use, and disclose communications-related information whenever a subscriber has consented. To be sure, there may be ambiguity in the terms of service of existing contracts. But there does not appear to be any barrier to cybersecurity information-sharing arrangements if they are, ultimately, grounded on the affirmative, opt-in consent of a customer.

Other Legal Issues: The Telecommunications Act, the Fourth Amendment, and Antitrust

Though the SCA and Wiretap Act are most often cited as grounds for limited information sharing, some critics also suggest that the Telecommunications Act of 1934, the Fourth Amendment to the Constitution, and the Sherman Antitrust Act may also set limits. On closer examination these arguments also seem to overstate the case.

The Telecommunications Act, which was substantially updated in 1996, requires service providers to maintain the privacy of customer proprietary network information—that is, information about a customer's use of the telecommunications network.[67] But the law has provider protection language that is arguably somewhat broader than that in either the SCA or the Wiretap Act. The Telecommunications Act exempts from the privacy requirements disclosures "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[68] Though little attention has been paid to this provision, it would seem to authorize the use of customer proprietary information to prevent a cyber intrusion because that would seem to be an unlawful and abusive action.[69] Here, too, routine disclosures may be impermissible. But the Telecommunications Act would not seem to be any greater barrier to sharing than the SCA or the Wiretap Act.

Some also worry that the Fourth Amendment might limit the ability of private sector actors to share information with the government. To be sure, if the government were

collecting information about the actions of an individual, it might be required to comply with the Fourth Amendment's limitations of particularity and reasonableness. But, those limitations apply only to government actors, not to private sector ones.[70] While it is true that private action may sometimes amount to government action when the private actor was serving as an instrument or agent of the government—for example, when a private employer performs drug testing mandated by government regulations[71]—that conclusion would be unlikely to apply to private sector ISPs that chose voluntarily to share information with the government or with each other.[72] Here, too, suggestions of illegality seem to be overstated.

Finally, some also argue that the Sherman Antitrust Act[73] applies to private-to-private information sharing. But the Act prohibits only information sharing that is an "unreasonable" restraint of trade.[74] It is difficult to imagine how sharing threat and vulnerability information would be considered a restraint of trade—indeed it is intended to have the opposite effect of fostering trade and commerce. The sort of information sharing at issue here is simply not equivalent to information sharing that may sometimes be used to fix prices. Perhaps if two major service providers agreed to share security information and purposefully excluded a third provider, with the intent of increasing their own market share, their action might be an illegal form of collusion. But absent that sort of agreement, neither law nor reason would seem to prevent information exchanges that would enhance cybersecurity. Here, again, the cautious response stems less from actual ambiguity in the law than from fear of something new and different.

So Why the Hesitation?

All of this leaves us with another puzzle: if the law does not prohibit the information sharing that both the public and private sectors say they want, why are they so hesitant and resistant to doing so effectively? On the government side, we have seen how resource constraints, a desire for accuracy over efficacy, and a cultural resistance to sharing classified information outside the government hamper the process.

In the private sector, the reasons are similar. Service providers and their lawyers are inherently cautious and want to avoid litigation and controversy at all costs. Likewise, there may be good business reasons why a service provider might prefer not to impose new terms of service on its clients in an overt way that engenders controversy. Seen in this light, complaints about the laws' ambiguity demonstrate the desire among companies for explicit legal protections from liability if they share information, and for relief from the ill will that might attend such a measure. Trying to avoid litigation and a difficult public relations battle are less persuasive reasons for failing to act, but they are nonetheless rational business judgments that may provide a good ground for legislation.

Thus far the private sector's bid for greater liability protection seems to have carried the political day. The salience of the information-sharing issue was highlighted by the recent proposal from the Obama administration for cybersecurity legislation. In the draft released in May 2011, the administration offered language to clarify that private sector actors (along with state and local governments) can share information about cyber threats or incidents with DHS. To address the private sector's concerns, the proposal would:

- Authorize private sector actors to share information with the federal government "for the purpose of protecting an information system from cybersecurity threats or mitigating such threats";
- Provide private sector actors with civil and criminal immunity for sharing cybersecurity information with DHS; and
- Preempt any inconsistent state or local law or regulation that would otherwise prohibit information sharing.[75]

While it is fine to attempt to resolve even latent ambiguity, the danger of the administration's proposal is the possibility it will fail. If Congress does not enact it, the implication will be that in the absence of explicit authorization, the contemplated information sharing is unlawful. Since a more nuanced analysis of the law indicates that this legal proposal is unnecessary in many situations, the residual implication could be pernicious.[76]

Perhaps of even greater concern, the draft proposal is silent on information sharing between private sector actors. By authorizing private-to-government information sharing to protect an information system, the law may be taken as prohibiting or limiting such sharing among private sector actors. That interpretation would be harmful. Despite this apparent problem, the exclusion of private-to-private sharing appears to have been the intent of the Obama administration. At a recent hearing, when asked why the preemption provision was not extended to private-sector exchanges—and in particular why no antitrust exemption was provided—the administration made clear that it had chosen not to do so for fear of reducing its own enforcement capabilities.[77]

Information Sharing and a Formalized Structure

Even if we accept the need for some solution to the ambiguity of current law, these and other similar legislative proposals have a certain inelegance to them. They take a body of existing law under the ECPA and other statutes and simply preempt it with a newer law. That brute force method only solves a portion the problem, for it does

not address the inherent limits on the government's willingness to share information with the private sector.[78] Indeed, one-sided legislative solutions enhancing private-to-government might not generate as much positive response as policymakers would hope.

In this regard the proposals seem to reinforce, rather than ameliorate, many of the criticisms leveled at the development and creation of sector-specific Information Sharing and Analysis Centers (ISACs). Since 1998, these centers—intended to foster the public/private sharing of threat and vulnerability information—have been created in most of the critical infrastructure sectors like financial services and chemical manufacturing, including the Information Technology ISAC.

The ISAC structure provides each sector with 24/7 information sharing and intelligence capabilities, allows the sector to collect and analyze threats based on its subject matter expertise, and coordinates with the government on sector-specific impacts. At best, the effort has been a moderate success. Industry often complains that the government is not effectively leveraging its capabilities and does not adequately share threat information in the cyber domain, usually for classification reasons. Though there have been no recent studies of ISAC effectiveness, one GAO review reports a number of breakdowns in information sharing.[79]

Partially in response to the inefficacy of the ICACs, the private sector has adopted its own private-to-private information-sharing model, known as the Industry Consortium for Advancement of Security on the Internet (ICASI). Founded by some of the largest private sector actors, including Cisco, Microsoft, Intel, and IBM, ICASI more or less replicates some of what the Federal ISACs do. It provides alerts about known vulnerabilities and has developed a common vulnerability reporting framework for use by the private sector that is perhaps more effective than the federal counterpart.[80] The ICACs and ICASIs create a habit of cooperation and allow greater mitigation of known threats.

Drawing on these examples, sound public policy might wish to facilitate even greater information sharing of this sort, through partnerships that are more comprehensive and holistic. One suggestion, about which I have written before,[81] is to formalize the public-private partnership necessary for cyber defense by creating a Congressionally chartered, non-profit corporation akin to the American Red Cross or the Millennium Challenge Corporation. We could call it the Cybersecurity Assurance Corporation (CAC) and give it authority to administer the creation and use of a public good: information about cyber threats.

Creation of such a corporation would address many of the concerns that have frustrated purely private or public responses. It would eliminate the "assurance"

and "free rider" economic problems by collectivizing the response. And it would allow greater maintenance of the security of classified information within the ambit of a government corporation. As a corollary, the quasi-public nature of the CAC could provide a forum in which defense-related, private-sector information could be shared without fear of compromise or competitive disadvantage. Thus the CAC would provide a secure platform that allowed the government and the private sector to fully utilize our information assurance capabilities and call on both public and private resources.[82]

At the same time, the quasi-private nature of the organization would provide greater assurance that legitimate concerns for privacy and government overreaching were suitably addressed. The centralization of the effort would allow for a unified and continuous audit of privacy compliance. The maintenance of a private-sector control structure would further insulate against misuse and abuse by governmental authorities. And the absence of return on investment concerns would allow the organization to focus on privacy protection and network integrity.

Such a course would not be without risks. For one thing, there is no reason to think that even this public-private corporation would be immune to issues of rent-seeking and regulatory capture. Perhaps of even greater concern, by creating a single focal point for cybersecurity efforts we risk creating a cyber Fort Knox: an attractive, high-value target of opportunity whose compromise would be catastrophic. By having a single focal point, we would also run a monoculture risk. In general, a diversification of defensive systems is preferable since it creates a "herd immunity" against attack by malicious actors through both software and hardware intrusions.[83]

A Caveat: Borders and the Law

Thus far we have examined only applicable federal laws. It is important to note that many state laws also apply to information sharing and are often more protective of privacy, and therefore more limiting of information sharing for security purposes, than federal laws. Likewise, the laws of other countries sometimes apply to Internet security and are highly variable and lack coherence. The result is an unfortunate balkanization of the essentially borderless domain of cyberspace.

The challenge is much like the one state law enforcement officials faced in attempting to prosecute Depression-era bank robbers. The perpetrators could escape investigation and prosecution simply by changing jurisdictions and hiding behind differing laws. The problem is best exemplified by Clyde Barrow's famous fan letter to the Ford automobile company, thanking it for providing the means by which he and Bonnie escaped justice.[84]

The solution, of course, was to federalize the crime of bank robbery and effectively eliminate the boundary problem. But what the U.S. government could do then with the stroke of a pen is much more complicated in the cyber context. A similar effort would require legislation to preempt certain state laws and harmonize rules of disclosure, of the sort the administration proposed earlier this year.

But even that may be insufficient to create incentives for private-sector information sharing given the continuing specter of international tort liability. And there is little prospect for near-term improvement on that front. In the international arena, liability protection for cooperating with governments, not to mention private-to-private sharing, will take years of work. Today we are just beginning to construct a transnational set of procedures for combating cyber crime. For the most part, information sharing across national boundaries is slow and limited—far more so than the nimbleness with which intruders can change their tactics. Indeed, our current system of transnational information sharing is positively archaic. Substantive convergence of the law is even farther off and may well prove impossible.

True Public Goods—Government as Protector

The theoretical model suggests another way to think about the government's role and the interaction with the private sector—one that removes the private sector from the equation. We might consider cybersecurity to be analogous to police services or national defense—that is, a public good the government can provide. Indeed, the analogy to police services may be quite apt, since the government provides baseline policing while private-sector actors are free to supplement the public sector's protections with their own private methods.

The Korea Internet and Security Agency (KISA) recently took steps that put that concept into practice.[85] Recognizing that small and mid-size businesses cannot afford expensive security systems, the KISA established a "Cyber Emergency Shelter"—a large group of servers staffed by security experts and equipped with extra-wide bandwidths and sophisticated security systems capable of warding off large-scale Distributed Denial of Service (DDoS) attacks. Small businesses were offered the shelter's services at no cost. Those who qualify and register were permitted to have their incoming traffic routed through the shelter for screening. In times of attack (KISA is especially sensitive to the possibility of North Korean action) those same businesses may "retreat" into the shelter and, presumably, be able to continue operations.

This program has intriguing possibilities. It certainly fits the framework of national cyber defense as a public good akin to police service, provided by the government and available to all, assuming the shelter is large enough to house all who need its

protection. It will, however, also maximize the Fort Knox effect previously noted: one can imagine no more attractive target to North Korean cyber warriors than the KISA cyber redoubt.[86] Nonetheless, if it is successful, the effort could be highly beneficial.

Where the Korean model translates national security as exclusively defensive in nature, another public goods model might also advance the concept of an "active defense," which is an offensive capability of some form. This is the theoretical model the Pentagon is contemplating.[87] So far the government's efforts have been limited to voluntary information sharing.[88] But one could readily imagine the government concluding that protecting critical infrastructure is too important to be left to the private sector.

Those sorts of efforts—in effect allowing DHS or NSA to deploy active defenses on the private networks—would raise a host of constitutional and policy problems. On the level of legal limitations, the government's inspection of private-to-private Internet traffic would raise significant Fourth Amendment concerns.[89] While much of the network traffic information is unlikely to be protected by the Constitution, network traffic inspection is not sufficient to fully protect the network.[90] Any operational system intended to prevent malicious intrusions must also inspect the packets of information containing highly personalized data, including the content of the information conveyed, because malware may reside anywhere in the packets distributed. Excluding the text of an e-mail from the domain of inspection as a matter of law would simply draw a road map showing malicious actors where to hide their malware.

To be sure, there is a plausible argument based on necessity: if the private sector efforts fail to secure the network, then the government must step in. And that argument of necessity might convince the courts that government monitoring of content on the Internet falls into that limited class of cases where some form of "special needs" allows for derogation from the Fourth Amendment's particularity and warrant requirements. If the program were couched in an administrative fashion without criminal sanction, it might pass constitutional muster.[91]

But even if lawful, such a program would require the resolution of a number of difficult and challenging policy questions: Should a government-operated Internet inspection system be run by the military or by the civilian organs of government? How would it be structured legislatively to protect privacy and civil liberties? What would be legitimate and illegitimate uses of the personal data examined and how long would that data be retained? And, perhaps most importantly, what oversight mechanism would be used to ensure that the program was operated lawfully and within its authorized parameters? The American public will be especially leery of any program that collects

personally identifiable information and subjects it to automated computer analysis.[92] In the end, the policy questions may prove intractable.

Managing Externalities—The Role of Government in Fostering Private Sector Cybersecurity[93]

As noted earlier, another element in the economics of cybersecurity is the recognition that many uses of cybersecurity goods have externalities—both positive and negative. Government can typically address these externalities by subsidizing those with positive effects while minimizing negative effects through taxation, regulation, or the imposition of liability. As I've said, there are reasons to be suspicious of any government effort to deal with externalities—both because of problems of regulatory capture and because of the government's inability to react nimbly enough to evolving cyber threats. But there are also reasons to think that the private sector cannot organize for its own self-defense and that the government's reliance on the private sector for its own connectivity demands its engagement.

Whatever the limits of the theoretical model, there is little doubt that, as a practical matter, some government engagement with the private sector is inevitable. The recent proposal from the Obama administration signals a heightened interest in affirmative government action and makes legislation distinctly more probable. What might a government program look like?

Nudging the Market: Incentives, Subsidies, and Disclosures

One alternative worthy of consideration is for the government to play an indirect role in nudging the markets toward more effective cybersecurity.[94] Rather than creating standards, the breach of which might result in liability, the government might work in partnership with industry to develop a set of recommended best practices for cybersecurity. It is possible that an independent certification industry would then develop and that insurance rates would follow compliance with those best practices.

The Obama administration's legislative proposal appears to be an effort in this direction—but it is so convoluted that it is more likely to result in confusion and dispute than to achieve the desired effects. The proposal[95] calls for DHS to take a significant regulatory role in managing cyberspace security in the private sector. Working with industry, DHS would identify certain critical infrastructure operators, presumably including both the Internet service providers and electric grid operators. DHS would help them develop a priority list of the most important cyber threats and vulnerabilities.

The infrastructure operators then would be required to develop their own plans for addressing the agreed-upon threats and vulnerabilities. A third-party, commercial

auditor would assess the implementation efforts, and some operators would also be required to report on their efforts to the Security and Exchange Commission and certify that their plans are sufficient—perhaps because inadequate cybersecurity could pose a financial risk of loss to investors. Third-party auditors responsible for assessing compliance would provide reports to the providers and to DHS. If DHS decided a security framework adopted by a critical infrastructure sector was not adequate, DHS would be authorized to work with the National Institute of Standards and Technology (NIST) to mandate a modified framework. Finally, DHS would be authorized to publicly identify critical infrastructure providers whose plans it deemed inadequate.[96]

This proposal creates a regulatory complex that would be difficult to administer. It would enshrine a structure of prioritization and regulatory development that would, inevitably, be far behind the technological curve of threats in cyberspace. And it holds out the prospect that the federal government will wind up dictating standards of security to a private industry that is far more nimble and innovative than the government ever can be.

While private sector cybersecurity can certainly be improved and is of vital interest to the federal government, it cannot come as a dictate from DHS and NIST. It can only be provided through collaborative public-private cooperation. The standard-setting aspects of this proposal may have some merit, but the enforcement mechanism leaves much to be desired.

Liability and Insurance: Unleash the Lawyers

Consider next the question of liability for negative externalities. One can imagine the development of a liability rule that would require service providers to pay for any harm caused by their failure to take reasonable protective actions. This would force software manufacturers and Internet service providers to internalize many of the negative costs they now externalize.

Theoretically, such a structure would have much to recommend it. Liability for tortious wrongs is a comparatively efficient method of modifying private sector behavior and does not require the government to set a constantly changing standard of conduct. Instead, the law simply requires that a provider take "reasonable" precautions. It leaves the articulation of what constitutes a reasonable precaution to the development of the common law.

More importantly, the creation of a liability system often naturally leads to the development of an insurance system against liability. The insurance function allows for a further spreading of risk in a way that fosters broad private-sector responsiveness.

With enough data, insurance companies routinely and efficiently price the comparative costs and benefits of preventative actions and require cost-effective measures as a condition of insurance. Indeed, in maturing markets, insurance companies often take the lead in setting reasonable standards of care—much as they did with the development of building and fire codes in the late nineteenth century.

But it may be exceedingly difficult to get from here to there. Insurance pricing is not feasible without both standards against which to measure conduct and liability that arises from failure to meet those standards. In the cyber domain, neither is currently available. There are no generally accepted cybersecurity standards and there is no generally applicable liability system in place to account for failures to meet those standards.[97] Despite the growth of some private-sector standard-setting initiatives like ICASI, private-sector actors are likely to be very unwilling to voluntarily create standards that lead to liability where none currently exist. As a result, the only sure way to create liability would be for the government to step in to set liability standards. Any such effort would also be fraught with political risk.

Regulation and Taxation

A more intrusive step would be to develop a traditional regulatory model of mandatory standards for cybersecurity—which would raise significant questions about government's ability to define the standards appropriately. It would also raise the routine problem of operationalizing regulatory mandates in a complex technical area. Even cyber-sophisticated governments like that of Estonia have been shut down because they did not know how to address threats and vulnerabilities and create doctrine about risk. How then would we define parameters to deal with these threats that could be mandated for the private sector?

Alternatively, the regulatory model could be followed in defining only outcomes, not operational standards. In this scenario, the government would define the desired outcome, such as appropriate reductions in data breaches or intrusions, and define the penalties for failure to meet those outcomes. Simply creating consequences also creates liability, and thus insurable risk, even in the absence of a mandate on how to achieve the desired results. As long as the desired results are not impossibilities, such as eliminating all intrusions, this would leave the private sector to determine the most cost-efficient means of achieving the public policy objective.

The final means by which government could incentivize private-sector activity is to use the tax code. If we tax an output or provide a tax credit/incentive for an expenditure, we create a financial incentive to act—one that history has shown to be fairly powerful in its ability to shape behavior. Though many believe that using the tax code to incentivize conduct can have unintended and undesirable consequences, and that our record of

using the tax code for incentives is poor, it nonetheless remains a tool by which our government has frequently sought to modify private-actor conduct. In this case, for example, Congress might consider a tax credit for qualifying expenditures on security systems as a way of pushing the private sector toward more security-conscious decisions. The result would be to subsidize positive behavior. Conversely, Congress could choose to tax activities with negative externalities. Here too, problems of government competence to regulate would arise.

Protected Networks

One critical forensic difficulty in combating cyber intrusions is the prevalence of anonymity on the Internet. This anonymity is inherent in the structure of the Interment and, in the long run, can only be changed by modifications to the existing Internet protocols established by the Internet Engineering Task Force (IETF).[98] While the entire Internet might be better protected by the development of identification protocols, the IETF's institutional resistance to such structural changes makes this highly unlikely—as does the widespread commitment of Internet users to a vision of Internet anonymity and freedom.

What is more likely, however, would be for the economic incentives to drive the market to create walled areas on the Internet with restricted membership—in effect adopting the "club goods" solution.[99] While these walled areas would offer greater security, they would come at the cost of limiting access to the information now available on the Internet by limiting the very openness that makes the Internet so valuable. In the near term, we can expect to see a continued effort by the federal government to develop and foster the use of trusted identities. We may even see some cyber service providers moving to set different terms and conditions of service for different classes of customers. All of these actions are likely to be voluntary in nature, with users agreeing to sacrifice unlimited access in the name of security. As with the imposition of liability, however, any mandate in this area that smacks of a national identification requirement to access the Internet will meet fierce political opposition and will likely be nearly impossible to achieve.

Conclusion

In World War II, as German bombs fell on British factories, the British government did not require each factory to build its own anti-aircraft defense system, complete with fighters, radar, anti-aircraft guns, and fire and medical emergency responders. Rather, defense of the nation's factories was left in the hands of the government, whose leader, Winston Churchill, saw their protection as an obligation of the national defense establishment.[100] Yet today, as we face a new but also similar sort of threat—cyber attacks, like aerial ones, can cover a great distance in a short time—the idea of making the national government exclusively responsible for providing national cybersecurity

seems quaint and utterly impractical. We can't imagine government "cyber fighters" deployed on the Internet; nor can we envision a government-sponsored data backup and recovery system.

Perhaps what we are experiencing is a systematic failure of analogies. Cyberspace is not really the same as air space. The responsibility of Internet service providers to manage the content on the Internet and screen for malicious software may be no more than the obligation a highway operator has to screen traffic on the highway: none at all. Nor are ISPs like airplane operators and other public carriers who can or should control access to their systems and exclude those who pose a threat.

In fact, cyberspace is unique. And the best way to correctly approach fundamental policy questions about the division of authority between government and private actors is to begin with a fundamental analysis of first principles.

Those economic principles suggest there is a clear but limited domain in which government action is both appropriate and required: that of fostering the sharing of cybersecurity information. As for the rest of the bundle of cybersecurity goods, we face a wicked problem. Private sector actions will doubtless create externalities that the market cannot account for and that cannot be effectively managed by a self-organizing private sector. But the prospect of government action to correct for those externalities raises the same traditional problems of regulatory capture that attend any government endeavor. More fundamentally, precisely because cyberspace is unique in its rapidly changing and path-breaking nature, we face the almost intractable problem of creating policy too slowly to be of any utility. Ultimately, then, the principle recommendation for government is to treat cyberspace like any patient with an ailment and "first, do no harm."

Acknowledgments

My thanks to the participants at the Hoover Koret-Taube Task Force on National Security and Law, whose helpful comments on an earlier version of this paper contributed to its improvement.

Notes

1 Michael Arrington, "Google Defends Against Large-Scale Chinese Cyber Attack," TechCrunch, January 12, 2010, http://techcrunch.com/2010/01/12/google-china-attacks.

2 Ellen Nakashima, "Chinese leaders ordered Google hack, U.S. was told," *The Washington Post*, December 5, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/04/AR2010120403347.html. Note: The author has an active security clearance and has, therefore, been directed to treat the released cables as remaining classified. In

repeating here this public report of the alleged contents of the WikiLeaks cable he has neither examined the cable itself nor visited the WikiLeaks site.

3 Ellen Nakashima, "Google to enlist NSA to help it ward off cyberattacks," *The Washington Post*, February 3, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html?hpid=topnews.

4 Roughly a year ago, when I was touring the cybersecurity operations center of a major U.S. systems integrator, someone there told me confidently that "we have everything the government has and more." Sadly, this same integrator has been in the news recently after suffering a significant intrusion.

5 The statement of Senator Dianne Feinstein (D-CA) at a Senate Judiciary Committee hearing in 2004 is typical: "I would also note that 85 to 90 percent of our nation's cyber-infrastructure remains under the control of the private sector." http://feinstein.senate.gov/04Releases/r-cyberterror.pdf. Likewise, Mishel Kwon, the former director of the U.S. Computer Emergency Response Team (US-CERT) has repeated this figure, noting in an interview "the high level of private ownership of critical infrastructure (between 85–90 percent)," http://blog.executivebiz.com/2010/02/mischel-kwon-cybersecurity-is-many-problems-on-many-different-levels. While many people with responsibility in the cyber area offer this figure as fact, it has a bit of an "urban legend" air about it and I am unaware of a comprehensive survey documenting the figure.

6 In his elegant and delightful book *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (New York: Oxford University Press, 2009), David G. Post explains not only how the Internet came to have its current architecture, but also why the very "dumbness" of the Internet made it such a vibrant agent for innovation.

7 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," 4 *Journal of National Security Law & Policy*, 63 (2010).

8 All computer programs, including those used in cyber intrusions, are written in a programming language, often known as a source code. That source code is then compiled into the binary language understood by computers. To execute the program, or code, the computer reads the directions of the compiled binary language. This complex rendering from source code to executable instructions makes reading lines of computer code effectively impossible. While different types of airplanes look functionally distinct from each other, computer code does not.

9 Thomas Hobbes, *Leviathan*, Ch. 13 ¶9 (1651). I am not, of course, the first to offer this analogy. Others have more colorfully likened action in cyberspace to the Wild West of America's frontier. *See* Michael Fertik and David Thompson, *Wild West 2.0: How to Protect and Restore Your Reputation on the Untamed Social Frontier* (New York: Amacom, 2010).

10 *See* US-CERT, "Monthly Activity Summary" (April 2011), http://www.us-cert.gov/press_room/monthlysummary 201104.pdf.

11 Michael Barrett, Andy Steingruebl, and Bill Smith, "Combatting Cybercrime: Principles, Policies and Programs," PayPal, April 2011. https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_Com batingCybercrime_WP_0411 _v4.pdf.

12 Internet Crime Complaint Center, "2010 Internet Crime Report," http://www.ic3.gov/media/annualreport/2010 _IC3Report.pdf. The IC3 is a cooperative enterprise of the FBI, the Bureau of Justice Assistance, and the National White Collar Crime Center.

13 Department of Justice Inspector General, "The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat," p. i, April 2011, http://www.justice.gov/oig/reports/FBI/a1122r.pdf.

14 William Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," 97 *Foreign Affairs* (Sept./Oct. 2010).

15 "The Cost of Cyber Crime," Detica, February 14, 2011, http://www.detica.com/uploads/press_releases/THE _COST_OF_ CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf.

16 Elinor Mills, "Study: Cybercrime costs firms $1 trillion globally," *CNet News,* Jan. 28, 2009, http://news.cnet.com/8301-1009_3-10152246-83.html.

17 "The Cost of Cyber Crime."

18 "Cost of Cyber Crime is not Science Fiction, Says Detica," *Information Age*, May 4, 2011, http://www.information-age.com/channels/security-and-continuity/company-analysis/1621903/cost-of-cyber-crime-is-not-science-fiction-says-detica.thtml.

19 Government Accountability Office, "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," GAO-07–705, June 2007. These figures are also broadly consistent with the estimate of $140 billion in annual losses made by Ferris Research, as reported in "Cybersecurity: Where is the Security?" May 12, 2010, http://www.milesstockbridge.com/pdfuploads/640_Miles_Cyberspace_092410.pdf. Phishing is the colloquial term used for trying to trick people into disclosing their identity and password.

20 "First Annual Cost of Cyber Crime Study," Ponemon Institute, July 2010, http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study(1).pdf.

21 *Combating Robot Networks and Their Controllers*, Unclassified Version 2.0, May 6, 2010, http://www.scribd.com/doc/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0. One of the authors of the report, Rafal Rohozinski, gave a colloquial talk on this study to the St. Galen Symposium in early 2011. *See* http://www.youtube.com/watch?v=DpRYXRNWka0&feature=youtu.be.

22 This is an immense amount of data. It is roughly one million gigabytes and the storage capacity to hold that much data must have cost several hundred thousand dollars.

23 A zero-day exploit is a new vulnerability that has never been exploited before. Hence there are no known patches for it and it works immediately (that is, on the "zeroth" day). A botnet is a network of computers controlled by a malicious third party without the owner's knowledge. They are controlled like "robots," hence the name botnet.

24 Christopher Drew and Verne G. Kopytoff, "Deploying New Tools to Stop the Hackers," The *New York Times*, June 17, 2011, http://www.nytimes.com/2011/06/18/technology/18security.html?_r=1&scp=1&sq=hackers%20symantec&st=cse.

25 *See* Ross Anderson, Rainer Bohme, Richard Clayton, and Tyler Moore, "Security Economics and the Internal Market," European Network and Information Security Agency, § 4.2, 2007. A comprehensive study commissioned by the agency and described in this report reached much the same conclusion when surveying the academic literature in Europe.

26 The draft language is contained in Sections 101 and 106 of the administration's May 2011 proposal, available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

27 *See* "Regulatory Framework for Electronic Communications in the European Union," European Commission, at 55 (Dec. 2009), http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

28 "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor, March 29, 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

29 The program operated by affecting the rate at which nuclear centrifuges spun. To produce uranium suitable for use in a nuclear bomb, the centrifuges must run at a constant rate of speed. Stuxnet caused the centrifuges to run at a highly variable rate, while falsely reporting to their operators that everything was in working order. *See* John Markoff, "Stuxnet Software Worm Hit 5 Industrial Facilities in Iran," The *New York Times*, February 11, 2011, http://www.nytimes.com/2011/02/13/science/13stuxnet.html?_r=1&scp=3&sq=stuxnet&st=cse.

30 William J. Broad, John Markoff, and David E. Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel," The *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&nl=todaysheadlines&emc=tha2.

31 I thank Joshua House, a student in my recently completed seminar on Cybersecurity Law and Policy, at George Washington University, for an excellent research paper on which I have relied for many of the sources in this analysis. *See* Joshua House, "Private Good, Public Good, or No Good?: The Law and Economics of Cybersecurity Policy," December 2010, on file with author.

32 *See* Paul Samuelson, "The Pure Theory of Public Expenditure," *Review of Economics and Statistics,* 36 (4): 387–389 (MIT Press, 1954); David Schmidtz, *The Limits of Government: An Essay on the Public Goods Argument* (Boulder, Colo.: Westview Press, 1991).

33 Eric A. Fisher, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Opinions,* p. 7 (Nova Science Publishers, 2009).

34 Benjamin Powell, *Is Cybersecurity a Public Good? Evidence From the Financial Services Industry*, 1 The Journal of Law, Economics & Policy, p. 498 (2005).

35 Bruce H. Kobayashi, "Private Versus Social Incentives in Cybersecurity: Law and Economics," in Mark F. Grady and Francesco Parisi, eds., *The Law and Economics of Cybersecurity,* p. 16 (Cambridge, Eng.: Cambridge University Press, 2006). I am assuming, here that information is a "good." Some have argued that in the absence of artificial intellectual property protections, information is not a traditional economic good. *See* Murray N. Rothbard, *Man, Economy, and State: A Treatise on Economic Principles* 1033 (Ludwig von Mises Institute, Scholar's Ed., 2d. ed., 2009).

36 Esther Gal-Or and Anindya Ghose, "The economic incentives for sharing security information," *Information Systems Research*, 16 (2), 186–208 (2005).

37 *See* Christopher J. Coyne, "Who's to Protect Cyberspace?" *1 Journal of Law*, Economics and Policy, pp. 475–76 (2005).

38 Kobayashi, "Private Versus Social Incentives." Less persuasively, Neal Katyal has argued that purchases of private security goods spread fear, thereby potentially increasing the crime rate. *See* Neal K. Katyal, "The Dark Side of Private Ordering: The Network/Community Harm of Crime," in *The Law and Economics of Cybersecurity*, p. 202.

39 *See* Gordon Tullock, "Public Choice," *The New Palgrave Dictionary of Economics Online* (2d ed. 2008), http://www.dictionaryofeconomics.com/article?id=pde2008_P000240&q=rational%20choice&topicid=&result_number=10.

40 I am indebted to Professor Harvey Rishikof, Chair of the American Bar Association Standing Committee on Law and National Security, for this wonderful image. Quoting him also illustrates the proposition in a self-referential way. Like many in Washington, Professor Rishikof also has a government affiliation. If I had wanted to identify him by that affiliation, he would have required a week or more to get the requisite clearances from other officials. As a private sector actor, he authorized reliance on his imagery immediately.

41 *See* Joseph S. Nye Jr., *Cyber Power* (Harvard Belfer Center, 2010), p. 15, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

42 "Net neutrality" refers to the requirement that Internet service providers be neutral in the way they treat content going across their networks. One objection to the neutrality requirement is that large-scale users, like those who provide streaming video, may crowd out smaller users who are just sending text e-mails, for instance, because of limited bandwidth. For this reason, some argue that a break from strict neutrality is necessary to more fairly distribute costs among users.

43 The classic exposition of this idea is Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge, Eng.: Cambridge University Press, 1990); *see also* Elinor Ostrom, "A General Framework for Analyzing Sustainability of Social-Ecological Systems," *Science* (July 2009), p. 325.

44 *See* James M. Acheson, *The Lobster Gangs of Maine*, (Hanover, N.H.: University Press of New England, 1988); Pamela Quinn Saunders, "A Sea Change Off the Coast of Maine: Common Pool Resources as Cultural Property" 60 *Emory Law Journal*, (2011) (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1701225.

45 There are some who suggest that the Internet's capacity for collaborative work (sometimes known as "crowdsourcing") makes it different in this regard. They point to the success of Wikipedia as an example of successful self-organization enabled by the interconnectedness of the Internet. This is intriguing but has yet to produce many practical cybersecurity successes. For one example of such a success, *see* William Jackson, "Working group finds a way to thwart Conficker worm, with little help from federal agencies," *Government Computer News,* Jan. 26, 2011, http://gcn.com/articles/2011/01/26/conficker-working-group-lessons.aspx.

46 Economic considerations also point to one other possible answer to the problem of cybersecurity—a solution sometimes known as "club goods." These are resources (like a club room or a movie theater) from which some users may be excluded but where access is controlled such that the resources are non-rivalrous (that is, not subtractable). In the cyberspace context, this would be the equivalent of creating a walled garden domain with a limited number of users.

47 Wicked problems are problems of social policy that are complex and interdependent. Because they come with incomplete and contradictory information and often changing solution requirements they are typically thought of as impossible to solve. The classic description is found in Horst Rittel and Melvin Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences*, vol. 4, pp. 155–169, (Elsevier Scientific Publishing Company, Inc., 1973), reprinted in Nigel Cross, ed., *Developments in Design Methodology* (location: J. Wiley & Sons, 1984), pp. 135–144 http://www.uctc.net/mwebber/Rittel+Webber+Dilemmas+General_Theory_of_Planning.pdf.

48 Network traffic information can relate to suspicious packets, including ports, protocols, and routing information; specific virus/other malware signatures; IP addresses; and the identification of particularly suspect domains or servers. Personally Identifiable Information (PII) includes more person-specific types of information such as identifying web sites accessed; times and locations of logins/account access; discrepancies in user names; or content of communications. It is typically related to a specific malfeasant activity (such as an attempted fraud, identify theft or the transfer of terrorist finances).

49 One important caveat is needed: Information sharing is no panacea. It can, and will, help in preventing attacks where the threat signatures are known. It is ineffective, however, in preventing "zero-day" attacks—those that are effective on the "zeroth day" because nobody knows about them. The parallel is the spread of disease: information sharing is the equivalent of a distributing a known, effective vaccine, but no amount of information sharing or vaccination can protect against a brand new cyber attack or virus.

50 Executive Order 13526, §1.2(a)(1) (defining "Top Secret" information), 75 Fed. Reg. 707 (Dec. 29, 2009). "Secret" information is that whose disclosure would cause "serious damage" to national security. *See* Ibid., §1.2(a)(2).

51 *See* "Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed," (GAO-10–628, July 2010), pp. 14, 16.

52 Ibid., pp. 16–17.

53 Ibid., p. 17.

54 To enhance the willingness of the private sector to share information with the Federal government, DHS has created the Protected Critical Infrastructure Information (PCII) program. Under this program (codified at 6 C.F.R. Part 29) private sector information shared with the government for the purpose of protecting critical infrastructure is not subject to FOIA, cannot be used in regulatory actions, and can be shared with other private sector actors only in limited circumstances when identifying information is minimized. 6 C.F.R. §29.8(e). But these limitations apply only to information that originates in the private sector and, from context, the concern expressed to the GAO plainly relates to government-originated materials.

55 Ellen Nakashima, "NSA allies with Internet carriers to thwart cyber attacks against defense firms," *The Washington Post*, June 17, 2011, http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_story.html.

56 It does so at a significant cost, however. Because of privacy and civil liberties concerns, the private sector will not share the malicious code that it captures and interdicts with the NSA, thereby diminishing the NSA's ability to develop security information as a public good.

57 The draft provisions of the "Department of Homeland Security Cybersecurity Authority and Information Sharing Act of 2011" are in the Obama administration's May 2001 draft cybersecurity legislation, pp. 20–30, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

58 Public Law 99–508, Oct. 21, 1986, 100 Stat. 1848.

59 Title I is codified at 18 U.S.C. § 2510 *et seq*. The original Wiretap Act was passed in 1968 as Title III of the Omnibus Crime Control Act.

60 Title II is codified at 18 U.S.C. § 2701 *et seq*.

61 18 U.S.C. §2702(b)(5), (c)(3).

62 *O'Grady v. Superior Ct.*, 139 Cal.4th 1423 (2006).

63 18 U.S.C. § 2511(2)(a)(i).

64 As a Department of Justice manual details, the Wiretap Act:

> grants providers the right "to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service." United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). . . . The exception also permits providers to monitor misuse of a system in order to protect the system from damage or invasions of privacy. For example, system administrators can track intruders within their networks in order to prevent further damage. *See* [United States v.] Mullins, 992 F.2d [1472,] 1478 [9th Cir. 1993] (need to monitor misuse of computer system justified interception of electronic communications pursuant to § 2511(2)(a)(i)).
>
> . . . .
>
> [P]roviders investigating unauthorized use of their systems have broad authority to monitor and disclose evidence of unauthorized use under § 2511(2)(a)(i), but should attempt to tailor their monitoring and disclosure to that which is reasonably related to the purpose of the monitoring. *See* United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975) (phone company investigating use of illegal devices designed to steal long-distance service acted permissibly under § 2511(2)(a)(i) when it intercepted the first two minutes of every illegal conversation but did not intercept legitimately authorized communications).

Searching and Seizing Computers and Obtaining Electronic Evidence Manual, ch. 4 (3rd ed. Sept. 2009), http://www.cybercrime.gov/ssmanual/04ssma.html.

65 Section 314 of the USA PATRIOT Act, may also apply when the private-to-private sharing is done by a "financial institution" (as defined in 31 USC §. 5312(a)(2)). Such institutions are immune from liability for sharing information with each other when, broadly speaking, the information is shared for the purpose of establishing or maintaining an anti-money-laundering program. *See* 31 CFR *Part* 103.

66 18 U.S.C.§ 2511(2)(c) (Wiretap Act); 18 U.S.C. §2702(b)(3) (SCA).

67 47 U.S.C. §222(c)(1).

68 47 U.S.C. §222(d)(2).

69 One of the few cases interpreting this provision allowed Ameritech to access and disclose customer data in order to examine the conduct of one of its own employees. *See Schmidt v Ameritch,* 329 Ill.App.3d 1020, 768 N.E.2d 303 (2002).

70 The principle is a long-standing one. *See Burdeau v. McDowell*, 256 U.S. 465 (1921); *Coolidge v. New Hampshire*, 403 U.S. 443 (1971); *Walter v. United States*, 447 U.S. 649 (1980).

71 *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989); *see also Board of Education v. Earls*, 536 U.S. 822 (2002) (private school teachers).

72 The same might not be true if legislation affirmatively required the private sector actors to share information with the government. Hence any mandatory screening and reporting requirement should be viewed with caution.

73 15 U.S.C. §1.

74 The so-called "Rule of Reason" was first announced 100 years ago. *See Standard Oil Co. of New Jersey v. United States,* 221 U.S. 1 (1911).

75 The language is in §245 of the draft submitted to Congress by the administration on May 12, 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

76 Though some, from the privacy perspective, criticize the proposal as authorizing routine sharing of data, others, from the security perspective, condemn it for not making information sharing mandatory (reasoning that many will opt out of a voluntary program). From this perspective, the administration's proposal may be seen as either a reasonable compromise or unreasonable fence-sitting.

77 Eric Chabrow, "Law Interfering with Cybersecurity: Antitrust Fears Give Businesses Pause to Cooperate on IT Security," June 24, 2011, reporting on testimony of Associate Deputy Attorney General James Baker, http://blogs.govinfosecurity.com/posts.php?postID=986.

78 Nor does it address the latent antitrust issues, to the extent they have any force.

79 *See* "Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities," (GAO-05–434 May 2005), p. 32. A slightly more recent study noted that successful integration was highly variable across the ISAC sectors. *See* "Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics," (GAO-07–39 Oct. 2006).

80 John E. Dunn, "Security consortium agrees common vulnerability reporting standard," *ComputerWorldUK*, May 23, 2011, http://www.computerworlduk.com/news/security/3281379/security-consortium-agrees-common-vulnerability-reporting-standard.

81 *See* Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (National Academies Press, 2010).

82 Appropriate legal structures might include mandatory reporting; anonymization of information given to the CAC; compartmentalization of information that cannot be anonymized; and the development of a penalty structure for the misappropriation of CAC-protected information.

83 The author pretends no expertise in the epidemiology of herd immunity. What little understanding he possesses comes from a few useful review articles, including Paul E.M. Fine, "Herd immunity: history, theory, practice" 15(2) *Epidemiologic Reviews* (1993), pp. 265–302. Notably, adoption of this approach is consistent with recent conceptual thinking suggesting that cybersecurity issues are analytically akin to public health problems. *See* IBM, "Meeting the

Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination," Feb. 2010, pp. 11–23; K.A. Taipale, "Cyber-Deterrence," Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global, 2010, Jan. 1, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045.

84 There is some doubt as to the authenticity of this letter, but it is too amusing not to cite, especially since the underlying jurisdictional issue was quite real. *See* Clyde Barrow to Henry Ford (Apr. 13, 1934), http://texashideout.tripod.com/fordletter.html.

85 I was first made aware of this program through a research paper submitted by a George Washington University law student for credit in my course on Cybersecurity Law and Policy. *See* Jihan Joo, "Cybersecurity Policy and Practices of the Republic of Korea," December 2010, on file with author. Since the original sources are in Korean, everything I know about this intriguing idea I attribute with gratitude to Mr. Joo.

86 Indeed, this model seems to be developing as the solution-set for similar problems globally. In the analogous realm of securing the Domain Name System (the addressing function that tells one where, for example, hoover.org can be reached) the trend is toward keeping the critical core authentication information on just three distributed servers (in San Jose, Singapore, and Zurich). John Markoff, "Internet Security Experts Introduce Secure DNS in Singapore," The *New York Times*, June 24, 2011, http://www.nytimes.com/2011/06/25/science/25trust.html?_r=1. Having three super-protected strongholds for all of the core authentication information is a bit like painting a figurative bulls-eye on the servers. And unlike Ft. Knox, where we have a pretty high degree of confidence that the physical security is adequate to the task, in the cyber realm, offense still beats defense every time.

87 *See* Lynn, "Defending a New Domain." He argues for active defenses and a military role in defending civilian networks.

88 "US Govt launches pilot cyber defense program with ISPs, defense firms," *International Business Times*, June 19, 2011, http://sanfrancisco.ibtimes.com/articles/165468/20110619/us-govt-launches-pilot-cyber-defense-program-with-isps-defense-firms-dib-cyber-pilot.htm.

89 By contrast, the government's inspection of packets arriving at its own portals is not constitutionally problematic. *See* Office of Legal Counsel, "Legality of Intrusion Detection System to Protect Unclassified Computer Networks in the Executive Branch," Aug. 14, 2009, http://www.justice.gov/olc/2009/legality-of-e2.pdf.

90 Network traffic information is, almost certainly, analogous to telephone switching information. Because that sort of addressing information is publicly disclosed by the consumer as a way of having his call completed or his e-mail delivered, the courts have concluded that the sender/receiver has no reasonable expectation of privacy and thus that the information is not subject to the Fourth Amendment's warrant requirement. See *Smith v. Maryland*, 442 U.S. 735 (1979).

91 The "special needs" doctrine has typically been applied in places like schools, where the governmental authorities stand in a paternal relationship to their citizens. *See New Jersey v. T.L.O*, 469 U.S. 325 (1985) on allowing warrantless searches of a student for cigarettes and marijuana. But it is equally likely, if not more so, that the courts will look at government-operated Internet inspection systems as if they were police narcotics inspection checkpoints on the highway—a dragnet approach contrary to the Fourth Amendment. *See Indianapolis v. Edmond*, 531 U.S. 32 (2000).

92 The most notorious such program was John Poindexter's analytical system known as Total Information Awareness. Though little more than an experimental construct, the concept was eviscerated by public reaction. *See* William Safire, "You Are a Suspect," The *New York Times,* November 14, 2002, http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html.

93 Portions of this section are derived from a previously published work: "National Security Threats in Cyberspace" (American Bar Association & National Strategy Forum 2009) [Rosenzweig, Workshop Rapporteur]. (Reprinted with permission.)

94 *See* Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (New Haven: Conn.: Yale University Press, 2008).

95 The details of the proposal are contained in the "Cybersecurity Regulatory Framework for Covert Critical Infrastructure Act," which was part of the package submitted to Congress by the administration on May 12, 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf. Some of the analysis in this subsection originally appeared in Paul Rosenzweig, "Obama Cybersecurity Proposal Flawed, But Fixable," The Heritage Foundation, Web Memo No. 3300 (June 2011).

96 This is a perfect expression of the irony posed by the balance between transparency and secrecy. On the one hand, few could doubt the good-government value of publicly naming sectors or companies that are performing poorly. On the other hand, in doing so, the government might as well paint a target on the figurative corporate forehead. The prospects are so disadvantageous that one suspects the authority to name will be useful mostly for its *in terrorem* effect of coercing behavior, rather than any practical value of disclosure.

97 With one exception: There is a liability standard increasingly applicable to a limited class of cybersecurity cases in which the data integrity of customer information is breached. *See* 15 U.S.C. § 6801 and 16 C.F.R. § 314.4(a)-(c). But this liability structure is not yet fully developed and applies to a problem—data and identity theft—which, while clearly troubling, may not rise to the level of a national security concern.

98 Nobody actually owns or operates the Internet itself. While private-sector and government actors own pieces of the cyber domain (various routers and nodes, for example) the actual rules for how the cyber domain works are set by the IETF, which is an "open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architectures and the smooth operation of the Internet." *See* "Overview of the IETF," http://www.ietf.org/old/2009/overview.html. This community operates by the promulgation of technical standards that become de facto operating requirements for any activity in cyberspace. Thus, some questions about cybersecurity necessarily require engagement with an engineering community that is both internationalist and consensus-oriented, characteristics that may be inconsistent with effective U.S. government action.

99 *See* Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, Calif.: RAND Corp., 2009).

100 My friend and former boss, Stewart A. Baker, is fond of this analogy and thinks it says much about how we should approach cybersecurity. *See* Stewart A. Baker, "Denial of Service," Foreign Policy (Sept. 30, 2011), http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service.

The preferred citation for this publication is
Paul Rosenzweig, "Cybersecurity and Public Goods: the Public/Private "Partnership" (2011)," in *Emerging Threats in National Security and Law*, edited by Peter Berkowitz, http://www.emergingthreatsessays.com.

About the Author

Paul Rosenzweig

Paul Rosenzweig is the founder of Red Branch Consulting PLLC, a homeland security consulting company. Rosenzweig formerly served as deputy assistant secretary for policy in the Department of Homeland Security. He currently serves as a professorial lecturer in law at George Washington University, a senior editor of the Journal of National Security Law & Policy, *and a visiting fellow at the Heritage Foundation. He is the coauthor (with James Jay Carafano) of the book* Winning the Long War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom *and author of the forthcoming book* Cyberwarfare: How Conflicts in Cyberspace Are Challenging America and Changing the World.

Koret-Taube Task Force on National Security and Law

The National Security and Law Task Force examines the rule of law, the laws of war, and American constitutional law with a view to making proposals that strike an optimal balance between individual freedom and the vigorous defense of the nation against terrorists both abroad and at home. The task force's focus is the rule of law and its role in Western civilization, as well as the roles of international law and organizations, the laws of war, and U.S. criminal law. Those goals will be accomplished by systematically studying the constellation of issues—social, economic, and political—on which striking a balance depends.

The core membership of this task force includes Kenneth Anderson, Peter Berkowitz (chair), Philip Bobbitt, Jack Goldsmith, Stephen D. Krasner, Jessica Stern, Matthew Waxman, Ruth Wedgwood, and Benjamin Wittes.

For more information about this Hoover Institution Task Force please visit us online at www.hoover.org/taskforces/national-security.

HOOVER INSTITUTION
STANFORD UNIVERSITY